CLAIMS

1. A method comprising:

receiving an event from a first security engine;

identifying a second security engine configured to utilize information contained in the event; and

communicating the information contained in the event to the second security engine.

2. A method as recited in claim 1 wherein the event identifies a type of security attack.

3. A method as recited in claim 1 wherein the event identifies an action performed by the first security engine in response to a security attack.

4. A method as recited in claim 1 wherein the first security engine and the second security engine are application programs.

5. A method as recited in claim 1 wherein the first security engine is an antivirus application program.

6. A method as recited in claim 1 wherein the first security engine is a firewall application program.

7. A method as recited in claim 1 wherein the first security engine is an intrusion detection application program.,

8. A method as recited in claim 1 wherein the first security engine is a vulnerability analysis application program.

9. A method as recited in claim 1 further comprising:

identifying a third security engine configured to utilize information contained in the event; and

communicating the information contained in the event to the third security engine.

10. A method as recited in claim 1 further comprising:

receiving an updated security policy;

identifying at least one security engine associated with the updated security policy; and

providing the updated security policy to the identified security engine.

11. A method as recited in claim 1 further comprising:

receiving a request for data from the first security engine; and

communicating the requested data to the first security engine.

12. A method as recited in claim 1 further comprising storing information contained in the event in a central location accessible to a plurality of security engines.

13. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1.

14. A method comprising:

receiving a security-related event from a first security-related application program;

identifying information contained in the security-related event;

identifying a second security-related application program associated with the information contained in the security-related event; and

communicating the information contained in the security-related event to the second security-related application program.

15. A method as recited in claim 14 wherein the first security-related application program is an antivirus application program.

16. A method as recited in claim 14 wherein the security-related event is associated with system state information.

17. A method as recited in claim 14 wherein the information contained in the security-related event includes data identifying a type of security attack.

18. A method as recited in claim 14 wherein the information contained in the security-related event includes data identifying an action performed by the first security-related application program in response to a security attack.

19. A method as recited in claim 14 further comprising:

receiving system state information from a third security-related application program; and

storing the system state information such that the system state information is accessible to the first security-related application program and the second security-related application program.

20. A method as recited in claim 14 further comprising:

identifying a third security-related application program associated with the information contained in the security-related event; and

communicating the information contained in the security-related event to the third security-related application program.

21. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 14.

22. A system comprising:

a first security engine associated with a first type of security attack;

a second security engine associated with a second type of security attack; and

an event manager coupled to receive events from the first security engine and the second security engine, the event manager further to identify information contained in the events and to identify at least one security engine associated with information contained in a particular event, and further to communicate the information contained in the particular event to the at least one security engine.

23. A system as recited in claim 22 wherein the information contained in the events identifies a type of security attack.

24. A system as recited in claim 22 wherein the information contained in each event identifies an action taken in response to a security attack.

25. A system as recited in claim 22 wherein the information contained in the events includes system state information.

26. A system as recited in claim 22 further comprising a third security engine coupled to the event manager and associated with a third type of security attack.

27. A system as recited in claim 22 further comprising a storage device coupled to the event manager, the first security engine and the second security engine, the storage device to store event information.

28. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

receive a first security-related event from a first service;

identify information contained in the first security-related event;

receive a second security-related event from a second service;

identify information contained in the second security-related event;

communicate information contained in the first security-related event to the second service; and

communicate information contained in the second security-related event to the first service.

29. One or more computer-readable media as recited in claim 28 wherein the first security-related event identifies a particular type of security attack.

30. One or more computer-readable media as recited in claim 28 wherein the one or more processors further store the information contained in the first security-related event and the information contained in the second security-related event for access by other services.

31. One or more computer-readable media as recited in claim 28 wherein the one or more processors further communicate information contained in the first security-related event to a third service.

32. One or more computer-readable media as recited in claim 28 wherein the first service is associated with a first type of security attack and the second service is associated with a second type of security attack.